적극적 침입 대응을 위한 에이전트 네트워크 구현 방안

신 원*·이경현**

Implementation of Agent Network for Active Responses against Intrusions

Weon Shin* · Kyung Hyune Rhee**

이 논문은 2005학년도 동명정보대학교 학술연구비 지원에 의하여 이루어진 것임

요 약

본 논문에서는 기존의 침입 대응 방안을 살펴보고, 기존 방안의 문제점을 해결하기 위한 한 방법으로 에이전트 시스템 기반의 새로운 개념의 에이전트 네트워크를 제안한다. 제안된 에이전트 네트워크는 다양한 고정형 및 이동형 에이전트를 도입하여, 침입 탐지를 수행하고 정보를 수집하며 적극적인 대응을 수행할 수 있다. 이를 통하여 갈수록 지능화되는 다양한 침입에 대해 적극적이고 능동적인 대응을 위한 새로운 방향을 제시할 수 있을 것이다.

ABSTRACT

In this paper, we investigate the problems of existing solutions for intrusion detection and propose an agent network based on stationary and mobile agents on agent system to solve them. The proposed agent network can detect intrusions, collect their information and execute active responses against intruders by introducing various stationary and mobile agents. It will show a new approach of active responses against more intelligent and distributed intrusions.

키워드

Stationary Agent, Mobile Agent, Agent Network, Intrusion Detection, Active Response

Ⅰ. 서 론

인터넷은 전 세계를 연결한 네트워크의 네트워크(Network of Network)로써 정보화 사회를 구성하는 중요 기간망으로 인식되고 있다. 현재 다양한 정보가 인터넷으로 전송되고 있으며 전자상거래도 급진전되고 있다. 그러나 정보 공유를 중시하는 현재의 인터넷은 구조적인 취약성으로 인해 정보화 사회에 심각한 위협을 줄 수 있는 위험성을 내포하고 있다. 이에 대해 여러 선진 기업은 정보보호 기술을 적용한 가상사설망(Virtual Private Network), 침입차단시스템(Firewall) 및 침입탐지시스템(Intrusion Detection System) 등의 다양한 방안 및 제품을 제시하고 있다[1].

그러나 인터넷의 폭발적인 보급에 따른 역기능으로 시스템 파괴, 중요 정보 유출 등을 위한 다양한 공격 기법 및 침입 기술이 등장·성장하고 있다[2][3]. 또한,

* 동명정보대학교 정보보호학과 전임강사
** 부경대학교 전자컴퓨터정보통신공학부 교수

접수일자 : 2005. 5. 4

네트워크 및 인터넷 기술의 발전과 함께 침입 기술이 날로 자동화, 조직화, 에이전트화, 분산화되고 있으므로 현재의 침입 기법뿐만 아니라 미래에 예상되는 침입에 대하여 효과적으로 대응하기 위해서는 통합된 보안 시스템을 기반으로 유연하고 개방적인 정보보호 시스템 구축이 필수적이다[3]. 이를 위해서는 통상적인 네트워크 환경 하에서의 단순한 호스트 기반의 침입 차단 및 탐지가 아니라 전체 네트워크 구성요소 모두가 유기적으로 협력하여 침입을 탐지하고, 침입의 유형을 분석한 후 보안 정책을 수립하고, 적극적으로 침입에 대응할 수 있는 새로운 네트워크 구조의 개념이 도입되어야 한다.

본 연구에서는 고정형 또는 이동형 에이전트에 기반하는 새로운 에이전트 네트워크를 제안하고 침입에 대해 적극적인 대응을 위한 네트워크 구조 정립을 그 목표로 한다. 이를 위하여 2장에서는 관련 연구로써 통합 보안 관련 기술에 대하여 설명하고, 3장에서는 적극적인 침입 대응을 위한 에이전트 네트워크를 제안하고, 4장에서는 에이전트 네트워크의 구현 방안을 제시하였다. 마지막으로 5장에서는 결론 및 향후 연구 과제에 대하여 논의하였다.

Ⅱ. 관련 연구

최근 정보보호 문제의 심각성으로 인하여 기존 조직 단위의 침입차단시스템 및 침입탐지시스템은 이미 한계를 가져왔고, 정보보호의 대상이 세밀화되어 조직 구성원의 각 정보와 개인의 권한까지도 관리해야하는 필요성이 증대되었다. 특히, 다양한 어플리케이션 등장으로 권한 부여 및 접근 제어 기술이 복잡해짐에 따라 다양한 요구사항이 발생하였다. 이러한 패러다임의 변화로 인하여 "통합보안 관리기술"이 등장하게 되었다[4].

통합보안 관리기술을 도입하면 통합된 관리자 인터페이스를 통한 전체적인 정보보호 정책 수립, 중앙의 통합 관리를 통한 정보보호정책의 무결성 보장, 정보보호정책 손상시 최근 상태로의 복구 기능, 에이전트를 통한 정책 제어의 유연성 및 확장성 확보, 보안 관리 정보 공유를 통한 보안 영역(Secure Domain) 형성 기능, 보안 관리의 자율성 및 안전성 확보 등의 장점을 얻을 수 있다. 현재 상용 제품으로써 가장 대표적인 통합보안 관리기술은 *Check Point Software* Technologies, Inc.의 OPSEC[5]과 Network Associates, Inc.의 Active Security[6]가 있다.

"OPSEC(*Open Platform for Security*)"은 *Check Point* Software Technologies, Inc.가 제안하고 있는 표준으로 300여 개의 보안 업체가 참여하고 있다. 침입차단시스템과 보안 관리 시스템들을 상호 연동한 자율적 보안 관리를 목적으로 SVN(Secure Virtual Network) 구조에서Firewall-1, VPN-1과의 연동을 통한 보안 환경을 제공한다. 일관되고 효율적인 보안 관리를 위한 정보보호 정책 관리, 로그 모니터링, 경보 발생 기능, 리포트 생성 기능을 제공한다. 그림 1은 OPSEC의 기본 구성요소를 보여주고 있다.

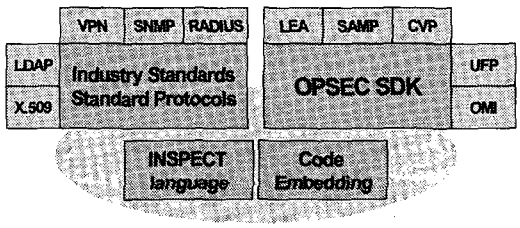

그림 1. OPSEC의 기본 구성
Fig. 1 Components of OPSEC

"Active Security"는 Network Associates, Inc.가 제안한 자율적 중앙관리 보안 모델로써, 보안 사건 및 문제점을 감시하고 진단하는 에이전트의 역할을 핵심으로 하여 사건 분석 및 대응 행동 양식을 결정한다. Active Security는 정보수집을 위한 Sensor, 시큐리티 정책 설정을 위한 Arbiter, 대응을 위한 Actor로 구성되어, Gauntlet Firewall, Gauntlet VPN Server, Event Orchestra 등의 자사 제품을 연결하여 보안 시스템을 통합하고 있다. 그림 2는 Active Security의 기본 구성요소를 보여주고 있다.

OPSEC과 Active Security는 각각 분산 통합 관리 및 중앙 집중 통합 관리의 서로 다른 접근 방식을 취하고 있으므로 어떤 방법이 더 효과적인지는 시스템 환경에 따라 다를 수밖에 없다. 또한, 두 방식 모두 자사 시스템을 중심으로 통합을 제공하고 있으므로 서로 다른 보안 시스템을 연동하는데 구조적인 한계가 존재한다[7].

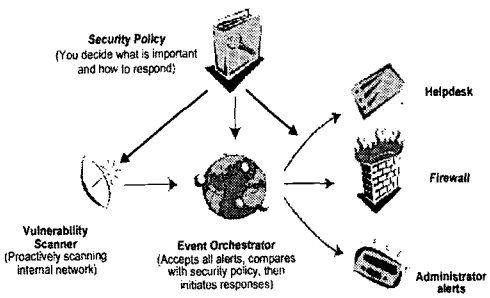

그림 2. Active Security의 기본 구성
Fig. 2 Components of Active Security

Ⅲ. 적극적 침입 대응을 위한 에이전트 네트워크의 제안

1. 에이전트의 정의

에이전트 네트워크를 구성하는 핵심인 "에이전트(Agent)"는 네트워크의 여러 곳에 위치하면서 다양한 측면의 정보를 수집하는 소프트웨어 모듈로, 네트워크 트래픽을 실시간으로 감시하여 악의적인 공격 행위를 탐지하고 이에 자동 대응을 목적으로 한다[8]. 즉, 네트워크를 거쳐가는 트래픽을 분석하고, 실시간으로 패킷을 모니터링함으로써 관리자가 설정한 규칙을 기반으로 위협을 탐지한다. 또한, 데이터 및 패킷을 분석하여 이미 저장된 데이터베이스의 탐지 패턴과 비교하여 일치할 때에는 미리 정의된 정책에 의해 상황에 따른 적절한 대응도 수행한다[7][9].

에이전트 네트워크 상에서 실행되는 에이전트는 동작 방식에 따라 하나의 호스트에서만 동작하는 "고정형 에이전트(*Stationary Agent*)"와 네트워크 상의 여러 호스트들을 이동하면서 작업을 수행하는 "이동형 에이전트(Mobile Agent)"로 구분할 수 있다[8]. 특히, 이동형 에이전트는 네트워크 상의 여러 호스트들을 이동하면서 트래픽을 감시하고 악의적인 공격 유무를 탐지하는 것을 목적으로 하는 에이전트이다. 따라서, 에이전트 보호를 위해 이동형 에이전트 시스템에서의 실행 환경 보호 및 에이전트 실행 보호를 위한 기술도 적용 가능하다[7][8].

2. 네트워크 에이전트의 분류

네트워크 에이전트는 그림 3과 같이 구성되고, 그 고유의 기능에 따라 다음과 같이 분류한다.

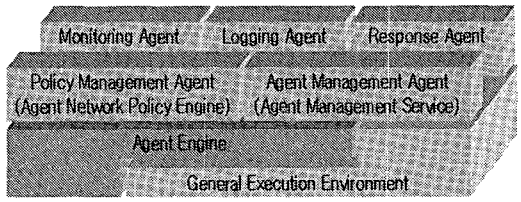

그림 3. 네트워크 에이전트 플랫폼
Fig. 3 Platform of network agent

2.1 에이전트 엔진(Agent Engine)

에이전트 동작을 위한 실행 환경으로, 각 에이전트들이 다양한 기능을 호출하여 사용할 수 있도록 별도의 API를 제공한다.

2.2 관리 에이전트(Management Agent)

다른 에이전트와 정책을 관리하는 에이전트이다. 에이전트 관리 에이전트(Agent Management Agent)는 주기적으로 호스트 상에 존재하는 다른 에이전트의 무결성을 검사하고 업그레이드를 담당한다. 정책 관리 에이전트(Policy Management Agent)는 수립된 정보보호 정책 전달 및 갱신을 위한 에이전트로써, 패킷 필터링 규칙, 접근 제어 리스트를 유지하고 모니터링 에이전트, 로깅 에이전트, 대응 에이전트에게 정책 정보를 전달한다.

2.3 모니터링 에이전트(Monitoring Agent)

네트워크 및 시스템의 동작을 감시하는 에이전트이다. 취약성 점검 에이전트(Vulnerability Scanning Agent)는 각 시스템 자원에 대한 취약성을 점검하고 레포트를 작성한다. 침입탐지 에이전트(Intrusion Detection Agent)는 데이터베이스화된 침입 패턴에 따라 침입을 탐지한다. 트래픽 분석 에이전트(Traffic Analysis Agent)는 네트워크 트래픽을 검사하는 에이전트로, 이상 트래픽 발견 시 이미 정의된 별도의 동작을 수행한다.

2.4 로깅 에이전트(Logging Agent)

로깅 에이전트는 각종 패킷에 대한 경로 정보를 관리하고 TCP 및 UDP 연결 로그 정보를 기록하는 에이전트로 패킷 로그 기록을 수행한다.

2.5 대응 에이전트(Response Agent)

네트워크 및 시스템 침입 발생시 그 대응을 목적으로 하는 에이전트이다. 접근 제어 에이전트(Access Control Agent)는 정책 관리 에이전트에서 전달된 정보보호 정책을 동적으로 반영하여 침입 대응을 수행한다. 역추적 에이전트(Tracing Agent)는 침입 대응 방식에 다른 역추적 프로토콜을 수행한다. 모니터링 에이전트 및 로깅 에이전트가 기록한 정보를 기반으로 침입자에 대한 역추적을 수행한다.

다음 그림 4는 침입 탐지 및 대응을 위한 에이전트 네트워크의 전체 구성 요소를 개략적으로 보여준다.

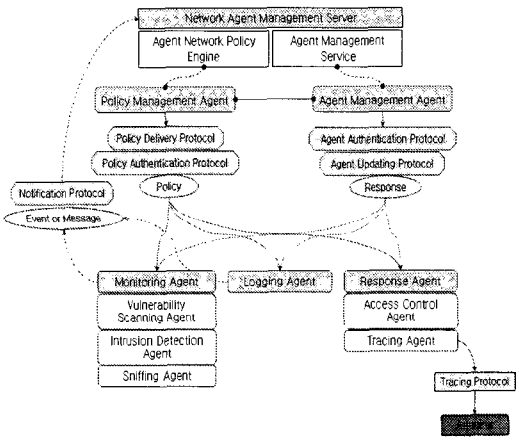

그림 4. 에이전트 네트워크의 구성 요소
Fig. 4 Components of agent network

에이전트 네트워크가 침입에 적절하게 대응하기 위해서는 기능적인 측면에 따라 다양하게 분류되어야 하는데, 그 이유는 다음과 같다. 첫째, 에이전트 네트워크는 침입탐지, 침입유형 분석, 대응의 절차에 따라 수행하므로 각 호스트에서 고유의 기능을 수행하기 위한 에이전트가 설치되어야 한다. 둘째, 각 호스트에 포함될 에이전트는 가능한 한 가벼워야 하고, 필수적인 기능만이 포함된 에이전트가 중요 위치에 설치되어야 한다. 셋째, 에이전트는 공격자의 일차적인 표적이 될 수 있으므로 여러 곳에 분산시켜 수행하면서 여러 정보를 공유할 수 있는 통신 구조를 가져야 한다.

3. 에이전트 네트워크의 동작 방식

에이전트 네트워크의 핵심은 각 호스트 상에서 동작하는 여러 에이전트들 간의 네트워킹 구조를 구성하고 이를 기반으로 상호 협력하여 네트워크 및 시스템 침입을 탐지하고 그에 대한 적절한 대응을 수행하는 것이다[7]. 본 절에서는 일상적인 동작과 침입이 탐지된 경우로 나누어 전체 에이전트 네트워크의 동작을 살펴본다.

3.1 기본적인 에이전트 네트워크 동작

시스템 시작

NAMS(Network Agent Management Server)는 관리 영역에 적절한 정보보호 정책을 수립하고 필수적인 에이전트를 준비하여 관리 에이전트를 통하여 호스트에 배포한다. 최초 초기화 과정에서는 다음과 같은 세부 사항들을 포함한다.

- NAMS의 에이전트 네트워크 정책 수립과 구현 에이전트 배포
  ① 각 에이전트 엔진을 대상으로 에이전트 관리 에이전트의 에이전트 갱신 프로토콜을 통한 에이전트 설치
  ② 각 엔진을 대상으로 정책 관리 에이전트의 정책 전달 프로토콜을 통한 정책 설치

침입이 탐지되지 않은 경우

각 호스트에 배포된 에이전트들은 다음과 같은 고유의 기능을 수행한다.

- 모니터링 및 로깅 에이전트의 고유 동작 수행
  ① 취약성 점검 에이전트는 주기적으로 해당 호스트에 대한 취약성 점검을 수행하고 NAMS에게 보고
  ② 침입탐지 에이전트는 주기적으로 해당 호스트에 대한 침입탐지를 수행하고 NAMS에게 보고
  ③ 트래픽 분석 에이전트는 주기적으로 해당 호스트에 대하여 비정상적인 네트워크 트래픽을 감시하고 NAMS에게 보고
  ④ 로깅 에이전트는 네트워크 상의 패킷 정보에 대한 기록 수행하고 주기적으로 NAMS에게 보고
- NAMS의 정보보호 정책 및 에이전트 코드에 대한 주기적인 무결성 검사
  ① 호스트 상의 에이전트 엔진을 대상으로 에이전트 관리 에이전트의 에이전트 인증 프로토콜을

통한 에이전트 무결성 검사

② 호스트 상의 에이전트 엔진을 대상으로 정책 관리 에이전트의 정책 인증 프로토콜을 통한 정책 무결성 검사

침입이 탐지된 경우

각 에이전트는 고유의 기능을 수행하다 침입이 탐지되면 그 사실을 NAMS에 보고한다. 침입 탐지시 에이전트 네트워크는 다음과 같이 동작한다.

- NAMS는 새로운 정보보호 정책 및 대응 수립
  ① 모니터링 에이전트 및 IDS에 의한 침입 탐지 후 NAMS에 보고
  ② NAMS의 로그 기록 및 탐지 유형을 분석한 후 새로운 정보보호 정책 및 대응 수립
  ③ NAMS 해당 영역의 에이전트의 무결성 검사 및 정보보호 정책 갱신
- 각 에이전트의 대응
  ① 접근 제어 에이전트의 해당 트래픽 차단 및 필터링 수행
  ② 역추적 에이전트의 로그 기록을 기반으로 한 공격자 역추적

3.2 침입에 대한 에이전트 네트워크의 대응

에이전트 네트워크가 침입에 대한 적절한 대응을 수행하기 위해서는 어떠한 유형의 침입이 발생하였는지 분류할 수 있어야 한다. 이를 위해 침입이 탐지되면 각 호스트의 취약성 점검 에이전트, 침입탐지 에이전트, 트래픽 분석 에이전트, 로깅 에이전트의 보고 자료에 따라 NAMS는 해당되는 침입 유형을 판단한다. 이를 기반으로 적절한 대응을 수립하고 정보보호 정책을 갱신한 다음 접근 제어 에이전트 및 역추적 에이전트를 동작시킨다.

다음 그림 5는 침입에 대한 에이전트 네트워크의 동작을 보여주는데, ①에서 침입 탐지 부분으로 침입인지 아닌지를 패턴 정보를 이용하여 판단하고, 침입이 확실하다면 ②에서 다양한 에이전트들로부터 정보를 수집하여 침입 유형을 분류한다. ③은 분류된 침입 유형에 대해 NAMS가 다양한 정보를 기반으로 대응을 수립한다. 최종적으로 ④에서 공격자가 속한 네트워크 및 공격자 시스템을 대상으로 다양한 정보를 수집하고 침입에 대한 증거 자료를 확보한다.

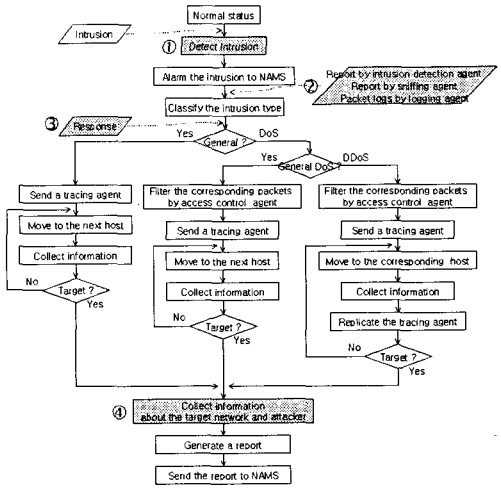

그림 5. 여러 침입에 대한 에이전트 네트워크의 대응
Fig. 5 Responses of agent network against intrusions

침입에 대한 에이전트 네트워크의 동작을 간략화하여 설명하면 다음과 같다.

일반적인 시스템 침입

각 에이전트는 침입이 탐지되면 그 사실을 NAMS에 보고한다. NAMS는 침입을 분석한 후 대응 정책을 수립하고 해당 네트워크의 에이전트들에 대한 무결성을 검증하고 해당 정책을 갱신한다. 각 대응 에이전트는 NAMS에서 수립된 정책에 따라 대응하고 그 결과를 보고한다.

서비스 거부 공격

먼저 NAMS는 네트워크 트래픽에 따라 일반적인 침입과 과도한 트래픽을 유발하는 서비스 거부 공격을 구분한 후, 트래픽 분석 에이전트의 네트워크 오버헤드와 로깅 에이전트의 패킷 로그 정보를 이용하여 대응한다. 서비스 거부 공격 시 대응은 일반적인 침입발생 시 대응과 유사하지만 접근 제어 에이전트를 이용하여 특정 트래픽을 차단하거나 필터링하는 점에서 다르다.

분산 서비스 거부 공격

NAMS는 패킷에 대한 로그를 분석하여 하나의 발신지에서 하나의 목적지로 다량의 패킷이 전송된다면 "단순 서비스 거부 공격"로 분류하고, 다수의 발신지로부터 하나 이상의 목적지로 다량의 패킷이 전송된

다면 "분산 서비스 거부 공격"으로 판정하여 대응한다. 또한, 서비스 거부 공격은 실제 시스템 침입을 위한 지원 공격이 되는 경우가 많으므로 효과적인 대응을 위해서는 비정상적인 트래픽에 대한 트래픽 분석 에이전트의 동작, 네트워크 패킷에 대한 로깅 에이전트의 동작과 함께 침입탐지 에이전트도 동작해야 한다.

Ⅳ. 구현 방안

최근 플랫폼 독립성을 장점으로 네트워크 개발 언어로 각광받고 있는 Java는 다른 언어로 개발된 라이브러리도 포함할 수 있는 JNI(Java Native Interface)를 제공한다[10]. JNI는 이름 및 호출에 대한 표준을 정의함으로써 JVM(Java Virtual Machine) 상에서 다른 언어로 개발된 원시 모듈을 적재하여 수행할 수 있도록 한다[10]. 즉, JNI를 통하여 JVM이 플랫폼 종속적인 입출력, 그래픽스, 네트워킹과 같은 로컬 시스템 호출을 수행할 수 있다. 따라서, 에이전트 네트워크의 하위 계층에서 시스템 종속적인 부분을 JNI를 통해 제어하고, 상위 계층에서는 Java 코드로 작성된 에이전트를 구현할 수 있다. 구체적으로 모니터링 에이전트, 로깅 에이전트, 대응 에이전트의 고유한 패킷 필터링, 패킷 로깅 등과 같은 플랫폼 종속적인 Platform Part는 C나 C++ 등으로 구현하고, JNI를 통하여 상위 계층으로 전달하면 Agent Part의 JVM에서 동작하는 이동형 에이전트인 관리 에이전트 등을 통하여 여러 에이전트 및 NAMS와 통신할 수 있게 된다. 그림 6은 이러한 동작 방식을 보여주는데, 여기서 HOST 1, HOST 2는 네트워크에 연결되어 JVM이 실행 가능한 환경이다.

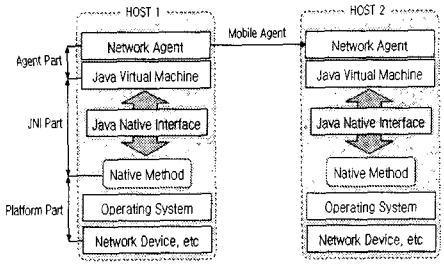

그림 6. 네트워크 에이전트의 내부 동작
Fig. 6 Internal operations of network agent

제안된 에이전트 네트워크는 네트워크로 묶여진 특정 도메인 내에 네트워크 에이전트 관리 서버 NAMS, 일반 사용자 컴퓨터(Host) 등으로 구성된다. 구현 방안에서는 실제 환경을 구성하기 위한 시뮬레이션 환경으로 NAMS를 LINUX 환경에서, Host는 Windows 2000/XP 환경에서 동작하도록 구성하였다.

```
class AgentManagementAgent
      extends MobileAgent{
   String agentID;
   Credential credential;
   Itinerary itinerary;
   int status;
   void migrate();
   void run();
   Credential getCredential();
   String getOriginator();
   String getCreator();
   String getPublicKey();
   String getPrivateKey();
   Date getTimestamp();
   String[] getHosts();
   int getStatus();
                  :
}
```

그림 7. 에이전트 관리 에이전트
Fig. 7 Java source of Agent management agent

에이전트 네트워크의 대표적인 이동형 에이전트인 에이전트 관리 에이전트의 구성은 에이전트 자체의 정당함을 증명하는 credential, 이동 경로가 포함된 itinerary, 이동을 실행하는 migrate(), 에이전트 관리 동작을 실행하는 run() 등을 가진다. 여기서, 에이전트 이동은 Java 객체 직렬화(Java Object Serialization)를 통한 소켓(Socket) 통신 또는 RMI(Remote Method Invocation)를 사용한다. 그림 7은 Java 클래스로 정의된 에이전트 관리 에이전트의 구성을 보여준다.

에이전트 네트워크에서 로깅 에이전트는 패킷 정보를 직접 다루므로 플랫폼 종속적인 패킷 정보를 JNI를 통해 구현한다. 제안 방안에서는 공개 패킷 캡쳐 라이브러리인 pcap[11]를 사용하여 패킷에 대한 실시간 정보를 로깅하도록 구성하였다. 다음 그림 8은 실제 동작을 보여 준다.

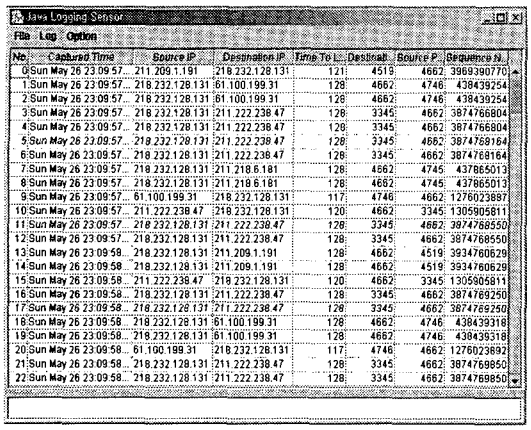

그림 8. 로깅 에이전트의 동작
Fig. 8 An Example of logging agent operation

그리고, 적극적 침입 대응을 위한 Java 기반의 에이전트 네트워크 구현을 위한 필수 기술 및 동작을 다음 표 1에서 정리하였다.

표 1. 에이전트 네트워크 구현 기술
Table. 1 Implementation technologies of agent network

		구현 기술	구분	동작
에이전트 엔진		JVM, Windows, Linux	실행 환경	에이전트 실행
관리 에이전트	에이전트 관리 에이전트	Java Code, JOS, RMI	이동형	서명 검증 에이전트 갱신
	정책 관리 에이전트	Java Code, JOS, RMI	이동형	서명 검증 정책 갱신
모니터링 에이전트	취약성 점검 에이전트	Java Code, JNI, C/C++	고정형	취약성 점검 리포트 기능
	침입탐지 에이전트	Java Code, JNI, C/C++	고정형	침입탐지 리포트 기능
	트래픽 분석 에이전트	Java Code, JNI, C/C++	고정형	트래픽 감시 리포트 기능
로깅 에이전트		Java Code, JNI, C/C++	고정형	패킷 로깅 연결 로깅
대응 에이전트	접근 제어 에이전트	Java Code, JNI, C/C++	고정형	정책 반영 패킷 필터링
	역추적 에이전트	Java Code, JOS, RMI	이동형	로깅 분석 패킷 역추적

V. 결 론

정보통신 기반 구축과 이를 기반으로 한 지식 기반 정보화 사회는 국가 경쟁력 및 위상을 높일 수 있는 획기적인 수단으로 세계의 수많은 국가들이 이를 성취하기 위하여 끊임없이 노력하고 있다. 그러나, 이러한 추세와 함께 정보화 사회의 역기능으로써 네트워크를 통한 시스템 침입 및 공격이 급격히 증가하고 있으며 최근에는 조직적인 사이버테러가 등장하고 있다[2][3]. 이를 방어하기 위하여 국가 차원에서 정보보호 기술을 기반으로 한 인터넷 정보보호 정책을 수립하고, 다양한 기업에서 침입탐지시스템 및 침입차단시스템이 개발되어 도입되고 있지만, 갈수록 지능화, 분산화, 조직화되는 시스템 침입 및 공격에 효과적으로 대응하기에는 현실적으로 어렵다[7]. 따라서, 이에 대응하기 위한 한 방안으로 시스템 침입에 대하여 네트워크 차원에서 보다 적극적으로 대응하는 개념인 "능동 보안"이 제안되었다[4].

본 논문에서는 능동 보안의 한 방안으로 적극적인 침입 대응을 목표로 고정형/이동형 에이전트로 구성되는 에이전트 네트워크를 제안하였다. 또한, Java 기술을 기반으로 필수요소인 네트워크 에이전트 방안과 구현 방안을 제안하였다. 이를 통하여 일반적인 시스템 침입, 서비스 거부 공격, 분산 서비스 거부 공격에 대하여 침입을 분석하고 보다 적극적인 대응을 수행할 수 있다.

적극적인 침입 대응 기술을 실현하기 위해서는 각 보안 시스템의 통합을 위한 상호 운영 기술 및 개방적인 시스템 구현이 필수적이다. 따라서, 이들을 위한 기술들을 종합적이고 유기적으로 연결할 수 있어야 하므로 각 요소 기술들이 균형적으로 발전해야 하고 전체적인 보안 기술 적용을 위한 상호 연동성이 반드시 보장되어야 한다. 즉, 능동 보안의 요소 기술들은 공격 탐지 및 대응 기술, 통신 프로토콜 기술, 능동 실행을 위한 플랫폼 기술, 인증 및 암호화 기술 등이 함께 적용 가능해야 하며 각 능동 노드 간의 상호 연동을 위한 공격 및 대응 기술을 위한 언어 설계, 안전한 이동형 에이전트 시스템, 인증 및 암호화 기술 등에 대한 연구도 심도있게 진행되어야 한다.

참고문헌

[1] 한국정보보호산업협회, "최신 정보보호 제품 및 기술 동향", http://www.kisia.or.kr/

[2] 인터넷침해사고대응지원센터, http://www.certcc.or.kr/

[3] 한국정보보호진흥원, http://www.kisa.or.kr/

[4] 한국정보처리학회, Active Network과 Security 기술 기반, Vol.1 No.1, 2000.

[5] OPSEC, http://www.opsec.com/

[6] Active Security, http://www.nai.com/

[7] 한국전자통신연구원, "능동 보안을 위한 이동형 에이전트 알고리즘 및 에이전트 네트워킹 구조 연구에 관한 연구" 최종보고서, 2002.

[8] 신원, "안전한 이동 에이전트 시스템의 설계와 응용", 박사학위 논문, 2001.

[9] C. A. Carver Jr., J. M.D. Hill, J. R. Surdu, and U. W. Pooch, "A Methodology for Using Intelligent Agents to provide Automated Intrusion Response", Proceedings of the 2000 IEEE Workshop on Information Assurance and Security, 2000.

[10] Java Technology, http://java.sun.com/

[11] TCPDUMP public repository, http://www.tcpdump.org/

[12] S. Fenet, S. Hassas, "A Distributed Intrusion Detection and Response System Based on Mobile Autonomous Agents Using Social Insects Communication Paradigm," First International Workshop on Security of Mobile Multiagent Systems, Autonomous Agents Conference, 2001.

[13] A. Dadon-Elichai, "RDS: Remote Distributed Scheme for Protecting Mobile Agents", AAMAS'04, 2004.

[14] A. T. Campbell et al, "A Survey of Programmable Networks", Computer Communication Review, Vol.29 No.2, pp.7-23, 1999.

[15] K. Psounis, "Active Networks: Applications, Security, Safety, and Architectures", IEEE Communications Surveys, First Quarter 1999.

[16] D. Denning, "Information Warfare and Security", Addison-Wesley, 1999.

[17] W. Jansen and T. Karygiannis, "NIST Special Publication 800-19: Mobile Agent Security," National Institute of Standards and Technology, 1999.

[18] C. M. King, C. E. Dalton and T.T. Osmanoglu, "Security Architecture: Design, Deployment and Operations", McCraw-Hill, 2001.

[19] D. J. Marchette, "Computer Intrusion Detection and Network Monitoring", Springer-Verlag, 2001.

[20] A. Menezes, P. van Oorschot and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, Boca Raton, FL, 1996.

[21] P. E. Proctor, "Practical Intrusion Detection Handbook", Prentice Hall PTR, 2001.

[22] B. Schneier, "Applied Cryptography", 2nd, John Wiley & Sons, 1996.

[23] W. Stallings, "Data & Computer Communications 6th Edition", Prentice Hall, 2000.

저자약력

신 원(Shin, Weon)

현 동명정보대학교 정보보호학과 전임강사

(주)안철수연구소 선임연구원

※ 관심분야 : 소프트웨어 보안, 악성코드 확산, 이동 에이전트 시스템, 암호 프로토콜 응용

이경현(Kyung Hyune Rhee)

현 부경대학교 전자컴퓨터정보통신공학부 교수

한국멀티미디어학회 학술이사
한국정보보호학회 논문지편집위원

한국전자통신연구소 선임 연구원
Univ. of Adelaide 응용수학과, Australia 방문교수
Univ. of Tokyo, 객원 연구원
Univ. of California at Irvine, USA, Visiting Scholar
Intergovernmental Organization, Colombo Plan Staff College, Manila, Philippines Chair of Division of Information & Communication Technology

※ 관심분야 : 정보보호론, 멀티미디어 정보보호, 네트워크 성능 평가, 그룹키 관리, 재시도 대기체계론